

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

In the Claims

1
2
3 1. (Currently Amended) A printer device comprising:
4 a data input device for receiving an encrypted digital document file;
5 a decryption algorithm for decrypting said received document file;
6 a controller for controlling printing of an image of data contained in said
7 received document file, wherein said controller operates to read quantity
8 permission data from said document file, said quantity permission data specifying
9 a number of copies of said document file authorized to be printed, and wherein
10 said controller operates to generate a confirmation message confirming receipt of
11 said document file; and

12 a printer mechanism for printing a physical copy of said document file,
13 wherein said controller operates to control printing of the number of copies
14 authorized to be printed, and after printing the number of copies authorized to be
15 printed of the document file, automatically deletes said document file from said
16 memory.

17 2. (Original) The printer device as claimed in claim 1, further comprising a
18 decryption key locally stored in said printer device.

19
20 3. (Original) The printer device as claimed in claim 1, comprising a
21 network interface for receiving said encrypted digital document file over a
22 network.
23
24
25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 4. (Original) The printer device as claimed in claim 1, wherein said
2 controller stores a unique device identification data uniquely identifying said
3 printer device, said controller operating to:

4 compare a received unique identifier data contained in said received
5 document file with said stored unique device identifier; and

6 if said received unique device identifier data differs from said stored unique
7 device identifier data, delete said document file.

8
9 5. (Original) The printer device as claimed in claim 1, wherein said
10 controller stores a unique device identification data uniquely identifying said
11 printer device, said controller operating to:

12 compare a received unique identifier data contained in said received
13 document file with said stored unique device identifier; and

14 if said received document identification data is identical to said received
15 unique device identifier data, control said print mechanism to print at least one
16 said physical copy of said document file.

17
18 6. (Cancel)

19
20 7. (Cancel)

S/N 10/056.117

Response to Office Action Mailed 09/11/2006

1 8. (Currently Amended) The printer device as claimed in claim 1, wherein
2 ~~wherein;~~

3 ~~said controller operates to generate a confirmation message confirming~~
4 ~~receipt of said document file;~~

5 said confirmation message comprises a time and date data, specifying a
6 time and date of receipt of said document file and a number of copies printed data,
7 specifying a number of copies of said document file physically printed by said
8 print mechanism.

9
10 9. (Currently Amended) A printer device comprising:

11 a data input device for receiving an encrypted digital document file;

12 a decryption algorithm for decrypting said received document file;

13 a controller for controlling printing of an image of data contained in said
14 received document file, wherein said controller operates to read a quantity
15 permission data content from said document file, said quantity permission data
16 specifying a number of authorized copies of said document file to be printed, and
17 wherein said controller operates to generate a confirmation message confirming
18 receipt of said document file; and

19 a printer mechanism for printing a physical copy of said document file,
20 wherein said controller operates to check a unique device identification data
21 contained in said document file with a stored unique device identification data of
22 said printer device, and provided a successful match is found, to print said
23 physical copy of said document file and to delete said document file after printing
24 said physical copy; and
25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 if said received unique device identifier differs from said storcd unique
2 device identifier data, said controller operates to delete said document file without
3 printing a physical copy of said document file.

4
5 10. (Currently Amended) A computer system configured for sending secure
6 encrypted document files, said system comprising:

7 a data processor;

8 a memory;

9 an encryption algorithm capable of encrypting a document file;

10 a device selector for selecting a said uniquely identifiable recipient device;

11 a file selector for selecting a document file;

12 a stored list of a set of authorized recipient devices, each said recipient
13 device identified by a unique device identifier data inaccessibly embedded within
14 said computer entity-system;

15 wherein said computer entity-system operates to:

16 select at least one document file, wherein the selected document file
17 comprises quantity permission data specifying a number of copies of said
18 document file authorized to be printed;

19 select at least one said uniquely identifiable recipient device to send
20 said document to:

21 encrypt said document files; and

22 address said at least one document file to said selected uniquely
23 identified recipient device; and
24
25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 at least one recipient printer device, said recipient printer device capable of
2 receiving an encrypted document file, establishing that said encrypted document
3 file is intended for said recipient printer device, generate a confirmation message
4 confirming receipt of said document file, decrypting and printing said encrypted
5 document file, and automatically deleting said document file after printing a
6 physical copy of a document from said document file.

7
8 11. (Previously Presented) The system as claimed in claim 10, further
9 comprising:

10 a network interface capable of sending said document file over a network to
11 said selected recipient device.

12
13 12. (Currently Amended) The system as claimed in claim 10, wherein:

14 said controller operates to read a quantity permission data content of said
15 document file, said quantity permission data specifying a number of authorized
16 copies of said document file to be printed; and

17 ~~said controller controls said printer mechanism such that said permitted~~
18 ~~quantity of physical copies of said document file are printed.~~

19
20 13. (Currently Amended) The computer system as claimed in claim 10,
21 ~~wherein said~~additionally comprising a user interface further displaysconfigured to
22 display:

23 data describing an encryption method used for sending said document.
24
25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 14. (Currently Amended) The computer system as claimed in claim 10,
2 ~~wherein said additionally comprising a user interface displays~~ configured to
3 display:

4 an acknowledgement message data describing receipt of said document file
5 by [[a]] said recipient device.

6
7 15. (Previously Presented) A distributed secure document printing system,
8 said system comprising:

9 at least one sending computer entity, capable of sending an encrypted
10 electronic document file, said document file having an encrypted data content, and
11 a unique device identifier data identifying a recipient printer device to which said
12 document file is intended to be printed by; and

13 at least one recipient printer device, said recipient printer device capable of
14 receiving said encrypted document file, establishing that said document file is
15 intended for said recipient printer device, decrypting and printing said document
16 file, and automatically deleting said electronic document file after printing a
17 physical copy of a document from said document file;

18 wherein said recipient printer device is configured to send a confirmation
19 message back to said sending computer entity, confirming receipt of said
20 document file, and confirming printing of a specified permitted number of copies
21 of said document file, wherein the specified permitted number of copies of said
22 document file is contained within the document file.

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 16. (Original) The system as claimed in claim 15, wherein said recipient
2 printer device is capable of reading a permitted quantity data content of said
3 document file; and

4 said recipient printer device operates for printing a number of physical
5 copies of said document file, corresponding to said permitted quantity data.

6
7 17. (Cancel)

8
9 18. (Previously Presented) A method of securely communicating an
10 electronic document file over a network, said method comprising the steps of:

11 encrypting said document file;

12 specifying a recipient device for sending said document file to, said
13 recipient device being uniquely identifiable by a unique device identifier data;

14 attaching said unique identifier data to said document file;

15 sending said document file in encrypted format to said intended recipient
16 device;

17 receiving said transmitted document file and decrypting said document file;

18 reading said unique device identifier data of said document file;

19 if said unique device identifier data of said document file corresponds to a
20 unique device identifier data of said recipient device, printing a physical copy of
21 said document file and automatically deleting said document file;

22 if said unique device identifier data of said document file does not
23 correspond with said unique device identifier data of said recipient device,

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 deleting said received document file without printing a physical copy of said
2 document file; and

3 sending, from said recipient device, a confirmation message back to said
4 sending computer entity, confirming receipt of said document file, and confirming
5 printing of a specified permitted number of copies of said document file, wherein
6 the specified permitted number of copies of said document file is contained within
7 the document file.

8
9 19. (Cancel)

10 20. (Cancel).

11
12 21. (Previously Presented) A method of secure printing of a received
13 document file, said method comprising the steps of:

14 receiving said document file in encrypted format at a receiving device;

15 decrypting said document file;

16 reading a unique device identifier data identifying a recipient device for
17 which said document file is intended;

18 comparing said unique device identifier data with a locally stored device
19 identifier data stored at said receiving device;

20 if said received unique device identifier data corresponds with said locally
21 stored device identifier data, printing at least one physical copy of said document
22 file and automatically deleting said document file;

23 if said received unique device identifier data differs from said stored unique
24 device identifier data, deleting said document file; and

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 sending, from said recipient device, a confirmation message back to said
2 sending computer entity, confirming receipt of said document file, and confirming
3 printing of a specified permitted number of copies of said document file, wherein
4 the specified permitted number of copies of said document file is contained within
5 the document file.

6
7 22. (Original) The method as claimed in claim 21, further comprising the
8 step of:

9 deleting said electronic document file, after printing said physical copy of
10 said document file.

11
12 23. (Original) The method as claimed in claim 21, further comprising the
13 step of:

14 reading a permitted quantity data describing a permitted quantity of copies
15 of said document file; and

16 printing said permitted quantity of copies of said document file.

17
18 24. (Original) The method as claimed in claim 21, wherein said document
19 file, after decryption is prevented from being viewed on a visual display device
20 prior to printing.

21
22 25. (Original) The method as claimed in claim 21, wherein said document
23 file is received via an intermediary carrier device having data storage capability.

24

25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 26. (Currently Amended) A method of sending a document file for printing
2 by a specified authorized recipient printing device, said method comprising the
3 steps of:

4 selecting a content of said document file;
5 encrypting said content;
6 attaching a unique device identifier data, identifying a recipient device to
7 which said document file is to be sent;
8 sending said document file to said recipient device; and
9 adding a permitted quantity data to said document file, said permitted
10 quantity data specifying a permitted number of copies of said document file which
11 can be ~~printed~~ printed; and
12 receiving a confirmation message confirming receipt of said document file.

13
14 27. (Cancel)

15
16 28. (Original) The method as claim in claim 26, further comprising the
17 steps of:

18 storing a document history data, said document history data specifying for
19 said document file:

20 a list of at least one recipient device to which said document file may
21 be sent;

22 a number of permitted copies of said document file which are
23 permitted to be printed by each said recipient device.
24
25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 29. (Currently Amended) A computer entity comprising a data processor, a
2 data storage device, a printer port, and having an attached printer device, said
3 computer entity comprising:

4 a module for decrypting an encrypted document file;

5 a unique device identifier for identifying said computer entity;

6 wherein said computer entity operates to:

7 receive a document file in encrypted format;

8 decrypt said document;

9 extract a unique device identifier data from said document;

10 compare said extracted unique identifier data with said unique
11 device identifier of said computer entity;

12 if a match is found between said received unique device identifier
13 data of said document and said unique identifier of said computer entity, send a
14 said document file for printing by said attached printer device; and

15 after sending said document to said printer device, delete said
16 document file from said computer entity; and

17 adding a permitted quantity data to said document file, said permitted
18 quantity data specifying a permitted number of copies of said document file which
19 can be ~~printed, printed;~~ and

20 receiving a confirmation message confirming receipt of said document file.

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 30. (Currently Amended) A method of secure printing of a received
2 document file, said method comprising the steps of:

3 receiving said document file in encrypted format;

4 reading a unique device identifier data identifying a recipient device for
5 which said document file is intended;

6 comparing said unique device identifier data with a locally stored identifier
7 data corresponding to a local computer entity device;

8 if said locally stored identifier data differs from said unique device
9 identifier data identifying said recipient device for which said document file is
10 intended, deleting said document file without printing any physical copies of said
11 document file; and

12 printing a number of physical copies of said document file, corresponding
13 to a permitted quantity defined in said document file, wherein the specified
14 permitted number of copies of said document file is contained within the
15 document file and wherein said document file is automatically ~~deleted~~.

16 and

17 sending a confirmation message confirming receipt of said document file.
18
19
20
21
22
23
24
25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 31. (Currently Amended) A method of secure printing of a received
2 document file, said method comprising the steps of:

3 receiving said document file in encrypted format;

4 sending a confirmation message confirming receipt of said document file;

5 reading a unique device identifier data identifying a recipient device for
6 which said document file is intended;

7 comparing said unique device identifier data with a locally stored device
8 identifier data;

9 reading a permitted quantity data describing a permitted quantity of copies
10 from said document file; and

11 if said received unique device identifier data corresponds with said locally
12 stored device identifier data, printing said permitted quantity of copies of said
13 document file and automatically deleting said document file; and

14 printing a number of physical copies of said document file, corresponding
15 to a permitted quantity defined in said document file.

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 32. (Currently Amended) A printer device comprising:
2 a data input device for receiving an encrypted digital document file;
3 a decryption algorithm for decrypting said received document file;
4 a controller for controlling printing of an image of data contained in said
5 received document file, for sending a confirmation message upon receipt of the
6 document file and for automatically deleting said document file; and
7 a printer mechanism for printing a physical copy of said document file,
8 wherein said printer device locally stores a decryption key for operating
9 said decryption algorithm to decrypt said received document file; and
10 wherein said printer device is configured to send a confirmation message
11 back to said sending computer entity, confirming receipt of said document file,
12 and confirming printing of a specified permitted number of copies of said
13 document file, wherein the specified permitted number of copies of said document
14 file is contained within the document file.

15
16
17
18
19
20
21
22
23
24
25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 33. (Currently Amended) A printer device comprising:
2 a data input device for receiving a digital document file;
3 a controller for controlling printing of an image of data contained in said
4 received document file and for sending a confirmation message upon receipt of the
5 document file; and

6 a printer mechanism for printing a physical copy of said document file,
7 wherein said controller operates to compare a received unique identifier
8 data contained in said received document file with a locally stored unique device
9 identifier data stored at said printer device and operates to control printing of a
10 predetermined quantity of said physical copy, wherein said predetermined quantity
11 is specified in said received document file;

12 if said received unique identifier data matches said stored unique device
13 identifier, control printing of at least one said physical copy of said document file
14 and automatically delete said document file; and

15 if said received unique identifier data contained the said received document
16 file does not match said stored unique device identifier data, to inhibit printing of
17 any physical copies of said document file.

18
19 34. (cancel)
20
21
22
23
24
25

S/N 10/056,117

Response to Office Action Mailed 09/11/2006

1 35. (Previously Presented) A printer device comprising:
2 a data input device for receiving an encrypted digital document file;
3 a decryption algorithm for decrypting said received document files;
4 a controller for controlling printing of an image of data contained in said
5 received document file; and
6 a printer mechanism for printing a physical copy of said document file,
7 wherein a decryption key is stored locally in said printer device for
8 operating said decryption algorithm to decrypt said received document files;
9 said controller operates to compare a received unique identifier data
10 contained in said received document file with a locally stored unique device
11 identifier data stored at said printer device;
12 if said received unique identifier data matches said stored unique device
13 identifier, control printing of at least one said physical copy of said document file
14 and automatically deleting said document file; and
15 if said received unique identifier data contained the said received document
16 file does not match said stored unique device identifier data, to inhibit decryption
17 of said document file and inhibit printing of any physical copies of said document
18 file;
19 wherein said printer device is configured to send a confirmation message
20 back to said sending computer entity, confirming receipt of said document file,
21 and confirming printing of a specified permitted number of copies of said
22 document file, wherein the specified permitted number of copies of said document
23 file is contained within said document file.
24
25